The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/14/2017

SUBJECT:
Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution (MS17-013)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Graphics Component, the most severe of which could allow for remote code execution if a user views a specially crafted web page or opens a specially crafted document. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Microsoft Windows: Vista, 7, 8.1, RT 8.1, 10
- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Windows Server Core Installations: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Office: 2007, 2010
- Microsoft Word Viewer
- Skype for Business 2016
- Microsoft Lync: 2010, 2013
- Microsoft Live Meeting 2007 Console
- Microsoft Silverlight 5 for Windows, Microsoft Silverlight 5 Developer Runtime for Windows

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**

- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Microsoft Graphics Component, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Multiple privilege escalation vulnerabilities exist when the Windows Graphics Device Interface (GDI) improperly handles objects in memory. (CVE-2017-0001, CVE-2017-0005, CVE-2017-0025, CVE-2017-0047)
- An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. (CVE-2017-0038)
- Multiple information disclosure vulnerabilities exist in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. (CVE-2017-0060, CVE-2017-0062, CVE-2017-0073)
- Multiple information disclosure vulnerabilities exist in the way that the Color Management Module (ICM32.dll) handles objects in memory. (CVE-2017-0061, CVE-2017-0063)
- Remote code execution vulnerabilities exist due to the way the Windows Graphics Component handles objects in memory. (CVE-2017-0108, CVE-2017-0014)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS17-013

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0001
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0005
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0014
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0025
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0038
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0047
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0060

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0061
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0062
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0063
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0073
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0108